# IN THE CLAIMS

**PLEASE AMEND THE CLAIMS AS FOLLOWS:**

1. (currently amended) A method of classifying a message, <u>comprising</u> ~~including~~:

determining the domain from which the message is purported to be sent;

determining an IP address from which the message was relayed at some point in [[its]] transmission <u>of the message</u>;

associating the domain with the IP address <u>to create an IP address and domain pair</u>; [[and]]

classifying the message ~~based on the~~ <u>using the IP address and domain pair based on one or more classification variables; and</u>

<u>assigning a score to the IP address and domain pair, the score comprising a ratio of a first classification variable to a second classification variable, the one or more classification variables decaying with time.</u> ~~associated domain and IP address~~[[.]]

2. (currently amended) The method of claim 1, further <u>comprising</u> ~~including~~ overriding a white list based on the classification.

3. (currently amended) The method of claim 1, wherein classifying includes ~~determining that the IP address is not commonly associated with the domain~~ <u>comparing the IP address and domain pair with a related IP address and domain pair</u>.

4. (currently amended) The method of claim 1, wherein classifying includes checking classifications of other messages associated with the [[same]] domain and different IP addresses.

5. (original) The method of claim 1, wherein a plurality of IP addresses is associated with the domain.

6. (original) The method of claim 1, wherein the IP address is associated with a plurality of domains.

7. (original) The method of claim 1, wherein the IP address is a boundary IP address.

8. (original) The method of claim 1, wherein the IP address is preconfigured.

9. (original) The method of claim 1, wherein the IP address is preconfigured to be one hop from a gateway IP address.

10. (original) The method of claim 1, wherein the IP address is learned.

11. (original) The method of claim 1, wherein the IP address is adaptively determined.

12. (cancelled).

13. (currently amended) The method of claim 1, wherein the IP address is a boundary IP address ~~determined according to claim 9~~.

14. (currently amended) The method of claim 1, <u>wherein determining the domain from which the message is purported to be sent includes identifying the stated sender domain associated with the message</u> ~~domain is the stated sender domain~~.

15. (currently amended) The method of claim 1, wherein the domain is [[the]] <u>a</u> ~~boundary~~ domain <u>associated with a boundary IP address</u>.

16. (original) The method of claim 1, wherein classifying includes consulting a white list.

17. (original) The method of claim 1, wherein classifying includes classifying the message based on previous classifications made to the IP address and domain pair.

18. (cancelled)

19. (original) The method of claim 1, wherein classifying includes determining a spam ratio.

20. (original) The method of claim 1, wherein classifying includes determining a spam rate.

21. (original) The method of claim 1, wherein classifying includes determining an estimated instantaneous spam rate.

22. (cancelled)

23. (original)  The method of claim 1, wherein classifying includes giving a classification greater weight relative to another classification.

24. (original)  The method of claim 1, wherein classifying includes giving a user classification greater weight relative to a computer classification.

25. (original)  The method of claim 1, wherein classifying includes giving an indeterminate classification a fraction of the weight of a good classification.

26. (original)  The method of claim 1, wherein classifying includes consulting a table indexed by IP address and domain.

27. (original) The method of claim 1, wherein classifying includes consulting a table indexed by IP address and domain wherein each cell includes information about previous classifications.

28. (currently amended) The method of claim 1, further ~~including~~ <u>comprising</u> providing [[the]] <u>a</u> ~~IP address and domain~~ classification <u>based on the IP address and domain pair</u> as input to another classifier.

29. (currently amended) The method of claim 1, further including providing [[the]] ~~IP address and domain~~ <u>a</u> classification <u>based on the IP address and domain pair</u> as input to a Bayesian classifier.

30. (original) The method of claim 1, wherein classifying includes classifying the message based on the IP address.

31. (original) The method of claim 1, wherein classifying includes classifying the message based on the domain.

32. (original) The method of claim 1, wherein classifying includes classifying the message based on the domain and determining that the message was forged.

33. (original) The method of claim 1, wherein classifying includes determining a score for the IP address.

34. (original) The method of claim 1, wherein classifying includes determining a score for the domain.

35. (currently amended) A computer -readable storage medium having embodied thereon a program, the program being executable by a processor to perform a method for classifying a message, comprising:

determining [[the]] a domain from which the message is purported to be sent;

determining an IP address from which the message was relayed at some point in [[its]] transmission of the message;

associating the domain with the IP address to create an IP address and domain pair; [[and]]

classifying the message ~~based on the~~ using the IP address and domain pair based on one or more classification variables; and

assigning a score to the IP address and domain pair, the score comprising a ratio of a first classification variable to a second classification variable, the one or more classification variables decayed with time ~~associated domain and IP address~~.

36. (cancelled)